REMARKS

Claims 1-3, 5, and 22-38 are pending in the application following entry of the foregoing amendment. Claims 1, 2, and 5 are amended to correct typographical errors. Claims 4 and 6-21 were previously canceled. New claims 22 and 23-38 are substantially similar to canceled claims 4 and 6-21, respectively. No new matter has been added.

Withdrawal of Allowable Subject Matter

Claim 4 was deemed in the previous Action to contain allowable subject matter. In order to facilitate prosecution in the response to the previous Action, claim 4 was cancelled, its elements were added to claim 1 from which it depended, and the remaining claims not dependent from claim 1 were canceled, mooting the rejection of those claims.

However, the indicated allowability of previous claim 4 stands withdrawn. Therefore, the subject matter of canceled claim 4 has been deleted from claim 1 and incorporated in new claim 22, and the subject matter of the other canceled claims has been incorporated in new claims 23-38. To facilitate prosecution, rejections contained in the previous Action with regard to that subject matter are addressed herein.

Claim Rejections - 35 USC § 103

Claims 1, 3, and 5 stand rejected under 35 USC § 103(a) as being allegedly unpatentable over Wiget (US 2004/0030804) in view of Rijhsinghani (US 6,112,251). Claim 2 stands rejected as being allegedly unpatentable over Wiget in view of Rijhsinghani as applied to claim 1, and further in view of McTernan *et al.* (US 2001/0034788). Applicant respectfully traverses these rejections.

To establish a *prima facie* case for obviousness under 35 USC § 103(a), it must be shown that the asserted references, when read alone or in combination, teach all of the elements of the examined claims.

The claims are directed to providing broadcast packet transmission capability to a logical network comprising a network segment having a "safe" broadcast domain, such as a wired network segment, as well as computing devices connected to the network segment via IPsec-based connections. IPsec connections require security associations (SA) to be set up. Setting up an SA involves authentication of the communicating parties. In the prior art, network broadcasting could not be used in conjunction with IPsec-based connections, because the broadcast address of a network segment did not identify anything that could be authenticated as required to set up an SA. The claims are directed to conveying all broadcast packets that should be sent over IPsec-protected connections through a gateway that acts as a broadcast relaying station. Broadcast packets on the network segment are duplicated and encapsulated by the gateway and forwarded individually to the appropriate IPsec-protected connections. Examples of such connections can include a secure wireless connection to a mobile workstation in a conference room, a remote computer securely coupled to the logical network through an outside wired network such as the Internet, and a secure connection to a remote gateway providing access to another wired network segment of the logical network. Each such connection has a security association (SA) set up with the gateway.

When the gateway receives a broadcast packet from the broadcast domain, it duplicates it into as many copies as there are SA-connected hosts, encapsulates each copy so that it can be sent over the SA for which it was created, and individually transmits each encapsulated copy over its respective SA-protected connection. Alternatively, when the gateway receives an encapsulated broadcast packet from an SA-connected host, it decapsulates the packet, recognizes it as a broadcast packet, forwards the packet to the broadcast domain, and duplicates and re-encapsulates it for transmission to any other SA-connected hosts.

In contrast to the claims, Wiget discloses a multi-cast enabled address resolution protocol (ME-ARP) that allows building IP based virtual private LAN segments (VPLS) over a multicast enabled IP backbone. Each VPLS has its own associated IP subnet. A customer premises equipment (CPE), such as a router, has one or more unnumbered virtual private network (VPN) internet protocol (UVIP) interfaces, each interface configured with a VPLS identifier and service IP subnet. In Wiget, "it is assumed that the providers of IP backbone services are IP multicast capable. Similarly, it is assumed that CPE devices are able to join a multicast group using IGMP." (paragraph [0028]). Each VPLS has a unique IP multicast address assigned. A UVIP interface of a CPE device, configured for a particular VPLS, joins the VPN's multicast group using IGMP. All broadcast traffic is then encapsulated and forwarded to the VPN's IP multicast address (paragraph [0036]). Thus, in Wiget, "IP multicast is used to forward broadcast [] traffic," (paragraph [0028] lines 9-10), and not point-to-point communication.

Unlike Wiget, the claims use point-to-point (i.e., unicast) communications to forward copies of broadcast packets to IPsec protected connections. The gateway receives a broadcast packet, and makes a copy of a broadcast packet for each host to which it has a connection through an established SA, encapsulates each copy for its respective intended host, and individually unicasts each encapsulated packet directly from the gateway to its recipient through the recipient's established SA. Thus, claim 1 has been amended to recite <u>unicast</u> transmitting the encapsulated broadcast packet through the IPsec-protected connection. Unicast transmitting the encapsulated broadcast packet is also recited in claims 2, 23, 26, 27, 30, 33, 34, and 36.

Rijhsinghani does not supplement Wiget to provide the recited unicast transmitting of an encapsulated copy of a broadcast packet through an IPsec-protected connection.

Because the asserted references, when read alone or in any possible combination, do not encompass within their scope nor teach all of the elements of independent claim 1, the 35 USC § 103(a) rejection of claim 1 is not supported, and claim 1 is allowable over the cited prior art. Claims 2, 3, and 5 depend from claim 1. Therefore, without prejudice to their own individual merits, those claims are also allowable over the cited prior art for at least the same reasons provided above with regard to claim 1.

Furthermore, with regard to the last clause of previous claim 1, (now deleted from claim 1 and included in new claim 22, similar to original claim 4), the examiner admits that Wiget does not disclose also transmitting data to unprotected connections, but contends that Rijhsinghani discloses providing a broadcast packet in secured and unsecured form (column 10 line 57 through column 11 line 8, reciting an encapsulated packet and an unencapsulated packet are sent). However, that is incorrect. The encapsulation of Rijhsinghani does not distinguish between secured and unsecured forms, as does the IPsec encapsulation of the claims. Instead, the encapsulation of Rijhsinghani merely serves to identify a LAN segment not connected directly to the LAN backbone, to which LAN segment a packet is sent. In Rijhsinghani, a broadcast packet is sent both to a so-called trunk station connected directly to the backbone, and to a LAN segment not directly connected to the backbone. The broadcast packet to be received by the trunk station does not need to be encapsulated, but the broadcast packet directed to the LAN segment must first be encapsulated to be received by the LAN segment.

With regard to claim 2, the examiner contends that McTernan discloses "duplicating broadcast packets (para. 41) to be sent to multiple destinations." However, that is not all that is recited in claim 2. McTernan at the cited location discloses a so-called Looping Data Sender which transmits packets in a repeating sequence, either to a multicast router or to a requesting client. If to a multicast router, the router transmits the data to all subscribing clients using ordinary multicasting. In contrast, claim 2 recites duplicating the broadcast packet into as many copies as there are IPsec-protected connections from the gateway computer to such parts of the logical network segment to which the broadcast packet should be transmitted, and encapsulating and unicast transmitting every duplicated copy of the broadcast packet to a respective IPsec-protected connection. McTernan does not disclose or suggest such an arrangement.

With regard to claim 3, the examiner contends in Wiget "a CPE device provides for a group of end stations [] and receives a copy of the broadcast packet for the end stations." However, that is not what is recited in claim 3. Instead, claim 3 recites "a bunch of currently existing IPsec-protected connections [] that end at a certain <u>same</u> receiving device," as described on page 16 line 25 to page 17 line 8 and shown in FIG. 12. Wiget does not disclose or suggest such an arrangement.

For these reasons as well, claims 2 and 3 are deemed allowable over the cited prior art.

Regarding claims 23, 26, 27, 30, 33, 34, and 36, the remarks made previously with regard to claim 1 are also applicable to those claims. Therefore, those claims are also allowable over the cited prior art. Claims 24-25 depend from claim 23, claims 28-29 depend from claim 27, claims 31-32 depend from claim 30, claim 35 depends from claim 34, and claims 37-38 depend from claim 36. Therefore, without prejudice to their own individual merits, those claims are also deemed allowable over the cited prior art.

Regarding claim 25, the remarks made previously with regard to claim 3 are also applicable to claim 25, and claim 25 is deemed allowable over the cited prior art for those reasons as well.

Conclusion

In view of the foregoing amendment and remarks, Applicants respectfully submit that the present application, including claims 1-3, 5, and 22-38, is in condition for allowance and an early notice of allowance is respectfully requested.

If the Examiner believes that any additional minor formal matters need to be addressed in order to place this application in condition for allowance, or that a telephone interview will help to materially advance the prosecution of this application, the Examiner is invited to contact the undersigned by telephone at the Examiner's convenience.

Respectfully submitted,

Santeri PAAVOLAINEN

By: ____________________
Gregory J. Lavorgna
Registration No. 30,469
DRINKER BIDDLE & REATH LLP
One Logan Square
18th and Cherry Streets
Philadelphia, PA 19103-6996
Tel: (215) 988-3309
Fax: (215) 988-2757
Attorney for Applicant